UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,541	12/26/2001	Robert Edward Moore	01.133.01	8301

7590 09/13/2005

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
BLUDAU, BRANDON S	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/025,541	MOORE ET AL.	
	Examiner	Art Unit	
	Brandon S. Bludau	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-30 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-30 is/are rejected.

7)☒ Claim(s) 1-10 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 26 December 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are informal and difficult to read. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

2. Claims 1-10 are rejected because the claimed invention is directed to non-statutory subject matter. A computer program is non-statutory subject matter when not disclosed in context of something tangible such as hardware.

also → clms 21-30 as an apparatus not comprising solely a non-statutory for being non-functional

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology

Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. Claims 1-5, 8-15, 18-25, 28-30 are rejected under 35 U.S.C. 102(e) as being anticipated by Kuo (US Patent 6230288).

4. As per claim 1, Kuo discloses a computer program product operable for controlling a computer to identify a computer file as potentially containing malware, said computer program comprising:

Searching code operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library (column 4 lines 15-27).

Context identifying code operable to identify a context within said computer file of said one or more target words (column 6 lines 54 –59); and

File identifying code operable if said context matches one or a predetermined set of contexts to identify said computer file as potentially containing malware (column 7 lines 35-38).

5. As per claim 2, Kuo discloses a computer program product as claimed in claim 1, wherein said predetermined word library includes one or more of:

Words that are names associated with known malware authors;

Words that are indicative of being part of a message embedded within said computer file by a malware author (column 4 lines 21-22);

Word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

Word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author.

6. As per claim 3, Kuo discloses a computer program product as claimed in claim 1, wherein said predetermined sets of contexts includes one or more of:

Within a script portion of a webpage;

Within a comment of a webpage;

Within executable code (column 6 lines 41 –44); and

Within a predetermined proximity to another target word.

7. As per claim 4, Kuo discloses a computer program product as claimed in claim 1, wherein, if said computer file is identified as potentially containing malware, then malware found code triggers one or more malware found action (column 7 lines 36-38).

8. As per claim 5, Kuo discloses a computer program product as claimed in claim 4, wherein said malware found actions include one or more of:

Quarantining said computer file;

Deleting said computer file;

Issuing a warning message concerning said computer file (column 7 lines 36 –38); and

Deleting a portion of said computer file suspect of containing malware.

9. As per claim 8, Kuo discloses a computer program product as claimed in claim 1, wherein all of said computer file is searched for said target words (column 4 lines 53-55).

10. As per claim 9, Kuo discloses a computer program product as claimed in claim 1, wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words (column 6 lines 41-44 where the predetermined contexts is executable code).

11. As per claim 10, Kuo discloses a computer program product as claimed in claim 1, wherein said malware comprises one or more of a computer virus, a worm and a Trojan. (column 4 lines 22 – 25).

12. Claim 11 is rejected because it discloses the same matter as claim 1.

13. Claim 12 is rejected because it discloses the same matter as claim 2.

14. Claim 13 is rejected because it discloses the same matter as claim 3.

15. Claim 14 is rejected because it discloses the same matter as claim 4.

16. Claim 15 is rejected because it discloses the same matter as claim 5.

17. Claim 18 is rejected because it discloses the same matter as claim 8.

18. Claim 19 is rejected because it discloses the same matter as claim 9.

19. Claim 20 is rejected because it discloses the same matter as claim 10.

20. Claim 21 is rejected because it discloses the same matter as claim 1.

21. Claim 22 is rejected because it discloses the same matter as claim 2.

22. Claim 23 is rejected because it discloses the same matter as claim 3.

23. Claim 24 is rejected because it discloses the same matter as claim 4.

24. Claim 25 is rejected because it discloses the same matter as claim 5.

25. Claim 28 is rejected because it discloses the same matter as claim 8.

26. Claim 29 is rejected because it discloses the same matter as claim 9.

27. Claim 30 is rejected because it discloses the same matter as claim 10.

Claim Rejections - 35 USC § 103

28. Claims 6-7, 16-17, 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kuo as applied to claim 1 above, and further in view of Chen (US patent 5960170).

29. As per claim 6, Kuo discloses the computer program product as claimed in claim 1, but does not disclose that if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

Chen does disclose that if said computer file is identified as potentially containing malware (column 12 lines 36-41), then a trigger threshold associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive (column 12 lines 41-46 wherein the trigger thresholds are more sensitive in that if a file is caught in the second scan it has a greater chance of being infected therefore the second scan is more sensitive).

Chen is analogous art because it discloses a method for virus detection.

It would have been obvious for one of ordinary skill in the art to modify Kuo to include a subsequent process that more sensitively detects viruses as shown in Chen.

Motivation for one to modify Kuo to include Chen would have been to reduce the computational resources needed to detect a virus as discussed in Chen (column 12 lines 50-53).

30. As per claim 7, Kuo discloses the computer program product as claimed in claim 1, but does not disclose that if said computer file is identified as potentially containing malware, then trigger thresholds associated with a heuristic malware identifying processes applied to said computer file is set to a more sensitive level.

Chen does disclose that if said computer file is identified as potentially containing malware (column 12 lines 36-41), then a trigger threshold associated with a heuristic malware identifying processes applied to said computer file is set to a more sensitive level (column 14-15 lines 58-16 wherein the virus detection module is considered a heuristic process by definition of heuristic, and whereas results of the scan are used to produce the virus detection module thereby increasing the sensitivity).

Chen is analogous art because it discloses a method for virus detection.

It would have been obvious for one of ordinary skill in the art to modify Kuo to include a subsequent process that more sensitively detects viruses as shown in Chen particularly a heuristic process.

Motivation for one to modify Kuo to include Chen as discussed above would have been to provide a method for detecting unknown viruses as discussed in Chen (column 14 lines 52-55).

31. Claim 16 is rejected because it discloses the same matter as claim 6.

32. Claim 7 is rejected because it discloses the same matter as claim 7.

33. Claim 26 is rejected because it discloses the same matter as claim 6.

34. Claim 27 is rejected because it discloses the same matter as claim 7.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau
Examiner
Art Unit 2132

BB

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100